



STARREVELD KOMT WEER UIT DE KAST

ADMINISTRATIEVE ORGANISATIE ALS GENERIEK KADER VOOR ACCESS CONTROL

Drs. André Koot RE CISM is redacteur van het blad Informatiebeveiliging en directeur-eigenaar van i3advies. Hij heeft 15 jaar ervaring op het gebied van Informatiebeveiliging en is auteur van diverse artikelen rondom Identity Management en Access Control. Hij is te bereiken via meneer@tken.net

Drs. Maarten Stultjens is werkzaam als VP business development bij Hunite in Alkmaar. Hij heeft ruim 10 jaar ervaring op het gebied van Identity & Access Management en Role Based Access Control. Hij is te bereiken via stultjens.maarten@gmail.com

Het toekennen en beheren van toegangsrechten kent de nodige uitdagingen. De belangrijkste vraag is op grond waarvan, op grond van welke principes, autorisaties aan individuen worden toegekend en beoordeeld. Zijn er normen en is hiervoor beleid geformuleerd? Dat geldt zowel bij het toekennen van autorisaties op basis van functies en rollen (denk aan RBAC of workflow) als bij het beoordelen van autorisaties door een manager of een IT-auditor.

Dit artikel tracht een generiek kader/framework te bieden om autorisatieregels op te stellen.

Generiek, omdat de ontwerpcriteria van toepassing zijn op iedere organisatie die haar eigen processen, objecten

en risico's kent. Hiervoor grijpen we terug op de oer-Hollandse begrippen die Starreveld heeft gedefinieerd in de leer van de Administratieve Organisatie.

Van Access Control naar Administratieve Organisatie en Starreveld

Organisaties streven naar het goed inrichten en controleren van autorisaties om reden van efficiency, beveiliging, voorkomen van fraude, goed kunnen ondersteunen van organisatieveranderingen enz... Voor veel organisaties is goed autorisatie-beheer zelfs een conditio-sine-qua-non, ze moeten voldoen aan wet- en regelgeving.

Het realiseren van autorisatiebeheer wordt in veel gevallen in één adem genoemd met het inrichten van identiteitenbeheer, Identity and Access Management, of I&AM. In de praktijk blijkt echter dat deze beide

aspecten maar zelden gelijktijdig ingericht kunnen worden. Sterker, het is eigenlijk wel een beetje vreemd dat

beide aspecten in één adem worden genoemd. Identiteitenbeheer richt zich op het lifecycle

management van identiteiten die binnen een organisatie kunnen worden gebruikt en dat is in de regel een HRM verantwoordelijkheid (voor eigen personeel) of een CRM taak (voor klanten en andere relaties). Dat proces heeft maar weinig te maken met autorisatiebeheer – het bepalen 'wie wat mag'. Dat laatste is een verantwoordelijkheid van proces- en gegevenseigenaren. Je zou hooguit kunnen stellen dat iemand zonder een vertrouwde, geaccepteerde identiteit geen autorisaties zou mogen bezitten. Het beheer van identiteiten is daarmee

dus wel een randvoorwaarde voor het kunnen inrichten van autorisatiebeheer, maar het is niet een onderdeel van autorisatiebeheer. In deze bespiegeling beperken we ons tot autorisatiebeheer, of Access Control.

Op grond van welke principes, worden autorisaties aan individuen toegekend?

Een leidend principe is werkverdeling

Met Access Control wordt bedoeld dat iemand die verantwoordelijk is voor een object (denk aan informatie, maar ook aan een fysieke kantoorruimte) in staat is te bepalen wie toegang tot dat object mag hebben en die ook toeziet op het (blijvende) juiste gebruik van de toegang tot het object. Dat omvat dan ook het soort autorisatie en de periode waarbinnen die autorisatie gebruikt mag worden. 'Wie mag wat wanneer'? Dat maakt echter al meteen duidelijk dat in ieder geval het eigendom van het te beveiligen object vastgesteld moet zijn. Iemand moet dit bepalen, afdwingen en controleren.

Waarom zou iemand autorisaties aan anderen toe willen kennen? Die laatste vraag is betrekkelijk eenvoudig te beantwoorden. Het leidende principe is werkverdeling en daarmee het beleggen van taken, bevoegdheden en verantwoordelijkheden bij iemand anders.

Als iemand geen werk hoeft te verdelen, dan is er ook geen probleem, denk aan de eigenaar/ondernemer met een eenmanszaak. Die persoon is integraal verantwoordelijk en hoeft eigenlijk alleen aan zichzelf verantwoording af te

leggen. Zo gauw echter de hoeveelheid werk te veel is voor één persoon, moet het werk georganiseerd worden.

Daarbij moet werk aan anderen worden toebedeeld en toevertrouwd (!) en ontstaat de noodzaak van het inrichten van beheersmaatregelen om de kwaliteit van het werk van die anderen te borgen.

Het invoeren van werkverdeling met beheersmaatregelen is niet nieuw. Het is bekend onder de noemer Administratieve Organisatie en Interne Controle en omvat onder meer het begrip Functiescheiding. Functiescheiding is een bekend begrip bij wet- en regelgeving, denk aan de beheersmaatregelen rond 'Segregation of Duties' in de Sarbanes Oxley traject. Het is een belangrijke factor geworden en het struikelblok waardoor menig organisatie bevindingen van toezichthouders heeft moeten wegwerken. In Role Based Access Control projecten bestaat dan ook veel aandacht voor inrichten van functiescheiding. Maar de bovenliggende vraag is: *"Op welke wijze kun je bepalen welke Taken, Bevoegdheden en Verantwoordelijkheden gescheiden moeten worden?"*.

Starreveld

We grijpen op zoek naar een antwoord naar de boekenkast met onze studieboeken over de leer van Starreveld – die in de jaren '60 de grondlegger was van de moderne Administratieve Organisatie (AO) en Interne Controle (IC). Uitgangspunt is dat een baas wil voorkomen dat zijn personeel fraudeert en de volledigheid van omzet kan worden gegarandeerd. Hij zal daartoe proberen om zodanige maatregelen te treffen dat fraude wordt ontmoedigd of tegengegaan en -in het geval het toch plaatsvindt- tijdig wordt gedetecteerd en getraceerd. Het ontmoedigen en tegengaan van fraude gebeurt op verschillende

manieren. Starreveld onderkent voor verschillende typologieën van organisaties, verschillende soorten beheersmaatregelen.

Starreveld ontwikkelde het gedachtegoed van functiescheiding

Zo ontwikkelde Starreveld instrumenten voor verbandscontrole (denk aan standen-registers bij verhuurders van onroerend goed en aan goederenbeweging bij handelsbedrijven: BeginVoorraad + Productie – Verkoop = EindVoorraad). Voor dit artikel beperken we de scope tot financiële transacties.

Ook ontwikkelde Starreveld het



Voorkomen van Fraude en Verduistering

gedachtegoed van functiescheiding door het creëren van tegengestelde belangen. Door het splitsen van bevoegdheden wordt voorkomen dat één persoon zoveel macht krijgt, of zoveel faciliteiten heeft dat hij of zij de bestaande beheersmaatregelen weet te omzeilen. Door het creëren van belangentegenstellingen wordt samenspanning van medewerkers, het samenwerken om beheersmaatregelen te omzeilen (ook in een situatie van functiescheiding), zo veel mogelijk tegengegaan. Maar helaas stelt ook Starreveld vast dat je samenspanning het moeilijkst van alle bedreigingen tegengaat.

Onze onderzoeksvraag is of, en zo ja hoe, de criteria van Starreveld voor functiescheiding te gebruiken zijn als generieke ontwerpcriteria voor autorisatiebeheer?

Functiescheiding

Het stelsel van Controletechnische Functiescheiding zoals gedefinieerd door Starreveld onderkent de volgende vijf 'functies':

- **Beschikken**
Beschikken impliceert dat je namens een bedrijf verplichtingen aangaat.
- **Registreren**
Dit is het vastleggen van een feit en heeft door automatisering een nauwe relatie met uitvoeren, zoals hieronder beschreven.
- **Uitvoeren**
Het uitvoeren van een taak conform de werkinstructie. Doordat veel systemen de processen geautomatiseerd ondersteunen, lijkt een strikte scheiding tussen uitvoeren en registreren niet meer helemaal van deze tijd.
- **Bewaren**
De functie die verantwoordelijk is voor kwaliteitscontrole (voldoet een object aan de gestelde normen) en het handhaven daarvan. Te lezen als Operationeel Beheer van een informatiesysteem.
- **Controleren**
Vaststellen of aan de vastgestelde normen wordt voldaan.



Stempelen en paraferen hielp vroeger

Starreveld geeft aan dat het borgen van de integriteit van informatie moet voldoen aan een aantal regels. Deze regels zijn kortweg als volgt: De controletechnische functiescheiding houdt in dat een zodanige

functie- en taakverdeling wordt gecreëerd dat:

- iedere functionaris slechts een beperkt aantal stappen van een proceskringloop kan beïnvloeden, maar nooit twee opeenvolgende;
- beslissingen om over waardevolle objecten te beschikken niet worden genomen door bewarende functionarissen;
- functionarissen die verantwoordelijk zijn voor de uitvoering van processtappen niet belast mogen zijn met de bewaring van objecten;
- de bovengenoemde functionarissen geen bemoeienis hebben met de activiteiten van de registrerende of controlerende functionarissen.

In onderstaande matrix zijn deze ontwerpcriteria op grond van de AO regels geformuleerd:

	Beschikken	Bewaren	Uitvoeren	Registreren	Controleren
Beschikkende functie	+	-	+	-	+
Bewarende functie	-	+	-	-	-
Uitvoerende functie	+	-	+	-	-
Registrerende functie	-	-	-	+	+
Controlerende functie	+	-	-	+	+
<i>Autorisatieregels</i>					

De groene combinaties zijn de in de praktijk goed te combineren functies. De rode combinaties zijn de verboden combinaties. We hebben deze matrix op grond van de voorgaande regels symmetrisch ingericht, maar door toepassing van compenserende en aanvullende maatregelen (zoals het automatisch vastleggen van audit-trails en inrichten van een workflow) zijn andere combinaties wellicht toch acceptabel.

Automatisering

De leer van Starreveld is ontstaan voordat sprake was van automatisering. Een heleboel functies en beheersmaatregelen die hij beschreef, zijn binnen de geautomatiseerde

bedrijfsprocessen eigenlijk niet meer als zodanig te onderkennen. Binnen de moderne geautomatiseerde systemen worden diverse functies geheel geautomatiseerd uitgevoerd. Met name de beschikkende en bewarende functies worden grotendeels geautomatiseerd uitgevoerd. Maar er zijn nog andere interessante ontwikkelingen. Daar waar vroeger een klant aan een loket verscheen of een brief stuurde, waarna een medewerker de relevante gegevens beoordeelde en registreerde in een dossier, neemt de klant nu zelf de registratie over in een webportaal en maakt de klant zelf al verschillende keuzes op grond van adviezen die een 'wizard' of intelligente assistent op de website presenteert. Hoe zit het dan met functiescheiding? Wie is dan nog verantwoordelijk voor de betrouwbaarheid van een transactie?

Starreveld kan ons hierbij toch wel helpen. De meeste door hem gedefinieerde functies kunnen we wel ergens onderkennen, al is het dan niet in een eenduidige vorm.

De beschikkende functie wordt bijvoorbeeld zichtbaar daar waar werkstroombesturing en kennisregels geautomatiseerd beslissingen nemen omtrent bijvoorbeeld acceptatie van een polis of een claim bij een verzekeraar. Of

daar waar een wizard of een intelligente assistent een aantal keuzes voorlegt aan een klant. De kennisregels zijn feitelijk de geobjectiveerde beslissingspunten die uitmonden in een transactie, een

feit waardoor een organisatie juridisch gebonden wordt. In die zin is een kennisregel (en de aan de beslissing ten gronde liggende parameters) eigendom van een iemand die een beschikkende functie moet vervullen. En die persoon is daarmee dan ook verantwoordelijk voor alle transacties die via deze kennisregels worden gerealiseerd.

De registrerende functie wordt ook steeds meer geautomatiseerd in portalen en wizards. De registratie gebeurt steeds meer aan de voorkant en dan noemen we dat 'data entry'. Het grootste risico is de integriteit van de ingevoerde gegevens, aangezien die in veel gevallen 'rücksichtslos' worden verwerkt in systemen. Verbandscontroles en plausibiliteitscontroles, evenals volledigheidchecks moeten zoveel mogelijk aan de voorkant worden ingericht. Daarmee wordt de proces-eigenaar verantwoordelijk voor de juistheid van de registratiefunctie. Willen we processen 'lean' inrichten, dan begint dat met juiste invoer.

De bewarende functie wordt in de regel door een systeem zelf uitgevoerd. Maar dat is natuurlijk al te simpel: de systeemeigenaar wordt hierdoor feitelijk de bewarende functionaris. Hij heeft tot taak de integriteit en vertrouwelijkheid, conform de eisen van de consumerende proces- en gegevenseigenaren te garanderen.

De kans op onbedoelde functie-vermenging zou in een geautomatiseerde omgeving kunnen ontstaan als een registrerende functionaris een geautomatiseerde beslissing initieert. Dus niet zozeer doordat hij zelf de beslissing neemt (dus beschikt) maar wel de gegevens invoert op basis waarvan een

systeem een beslissing neemt! Dit risico moet worden beperkt door bij het ontwerp en realisatie van de werkstroom en de kennisregels expliciet vast te stellen welke gegevens

Door automatisering
ontstaan nieuwe processen



Oogtoezicht kan nu niet meer

op welke wijze de beslissing hebben beïnvloed en door die beslissing in een audit-trail (wie heeft wat wanneer gedaan) vast te leggen voor controle achteraf. En bovendien: wie heeft de kennisregel goedgekeurd, wie is dus feitelijk 'accountable' voor de genomen beslissing?

Preventief en detectief autorisatie-beheer

Voordat we kunnen bepalen wat de waarde van 'Starreveld' is voor autorisatiebeheer, onderscheiden we allereerst twee methoden: preventief en detectief beheer van autorisaties. Preventief betekent dat uitsluitend op basis van vooraf gedefinieerde bedrijfsregels autorisaties worden toegekend. Preventief autorisatiebeheer wordt veelal ingericht met een combinatie van rollen (verzameling van autorisaties), regels (condities waaronder een rol kan worden toegewezen aan een gebruiker), context (eventuele veranderende omgevingsomstandigheden) en workflow (handmatige goedkeuring). We bekijken het voorbeeld van een medewerker op de afdeling debiteurenadministratie. Deze medewerker krijgt een standaard set autorisaties op grond van een 'rol' die past bij zijn functie. Als hij door zijn manager belast wordt met een

specifieke taak binnen de afdeling, krijgt hij hiervoor via een workflow extra autorisaties toegewezen voor een bepaalde tijd. De daadwerkelijke uitvoering van het autorisatiebesluit in autorisatieregels heet in IT-terminen provisioning en kan handmatig of via automatische interfacing worden gedaan. Voor preventief autorisatiebeheer wordt vaak verwezen naar Role Based Access Control (RBAC).

Detectief beheer van autorisaties is post-factum, dat wil zeggen dat het zich richt op het controleren van de huidige autorisaties tegen actueel geldende bedrijfsregels. Verkeerde autorisaties worden vervolgens opgeschoond of er wordt expliciete toestemming gevraagd om af te wijken van de geldende regels (certificatie of management verificatie). Als een als onjuist gesignaleerde toegekende autorisatie toch juist blijkt, dient de bedrijfsregel te worden aangepast. Voor detectief autorisatiebeheer wordt vaak verwezen naar Access Governance (AG). AG richt zich niet op het operationele proces van het uitdelen van autorisaties. Access Governance richt zich ook niet op het toetsen van de juistheid van de uitgevoerde transacties ten opzichte van een baseline.

Hoewel preventief beheer vanuit vele oogpunten te prefereren

is, blijkt het invoeren ervan een lastig traject omdat de organisatie de autorisatieregels vooraf moet definiëren en ze ook correct moeten zijn. Verkeerde regels leiden tot verkeerde autorisaties die bovendien vaak niet achteraf gesignaleerd kunnen worden en daarmee zouden kunnen leiden tot een onwerkbaar situatie, denk aan strakke preventieve autorisaties op een medisch dossier dat voor een spoedgeval toch geopend moet worden. Daarbij laten ongestructureerde omgevingen, zoals bestandssystemen of data in SharePoint, zich lastig structureren als onderdeel van een autorisatieproject.

Doordat detectief autorisatiebeheer minder impact heeft op de bestaande processen en IT-componenten is, is het ook sneller in te voeren. Met name organisaties die autorisatiebeheer snel onder controle moeten krijgen en snel moeten kunnen aantonen dat ze voldoen aan wet- en regelgeving kiezen voor deze AG-methode. IT-auditors passen bij audits eveneens AG-methoden toe. Door toepassing van deze methode worden niet alleen autorisaties opgeschoond, maar ontstaat tevens kennis over de rollen en regels. Deze kennis vergemakkelijkt de latere invoering van preventief autorisatiebeheer, bijvoorbeeld door 'normaal gedrag' uit te werken in een Role Mining project ten behoeve van RBAC.

Starreveld's waarde voor autorisatieregels

Een groot voordeel van de huidige tijd is wel dat we kunnen automatiseren. En dat kan omdat we steeds meer gaan standaardiseren. Daar waar Starreveld bijvoorbeeld handmatige controles moest uitvoeren, kunnen we dat nu grotendeels automatiseren. Het wordt nu zelfs mogelijk om realtime te controleren op afwijkingen van de gestelde norm. We kunnen realtime de juistheid en volledigheid van transacties controleren en dus vaststellen of de transactie door

en namens de juiste persoon is uitgevoerd en of de juiste autorisaties werden gebruikt. Het detectieve autorisatiebeheer levert in de huidige landschappen een goed instrument op om de verantwoordelijke functionaris de waarborg te bieden dat processen lopen zoals ze moeten lopen.

Door automatisering ontstaan wel nieuwe processen. Denk aan het toekennen van autorisaties en het ontwikkelen van autorisatieregels en -matrices. Het toekennen van autorisaties op basis van autorisatieregels is te beschouwen als een beschikkende functie. Het aanbrengen van wijzigingen in de autorisaties (provisioning) is een uitvoerende taak. Voor identiteiten-beheer onderkennen we met name registrerende en bewarende functies. Als ook op dat vlak de juiste beheersmaatregelen worden getroffen, is het ook beter mogelijk om op dat vlak 'in control' te zijn.

Aanbeveling

Dat alles betekent dat voor elk proces onderzocht moet worden welk soort functie door welk soort functionaris (of door welk proces) wordt uitgevoerd en dat de autorisatieregels conform de beslistabel moeten worden vastgelegd. Dat geldt niet alleen voor de bedrijfsprocessen, maar ook voor de autorisatie- en provisioning processen. Het eenduidig vastleggen van deze beleidslijn en de afzonderlijke regels is een belangrijk onderdeel van Access Governance.

Access Governance blijkt in de praktijk een effectieve en efficiënte methode om inzicht te verkrijgen in de juistheid van de aanwezige autorisaties en daarmee te voldoen aan wet- en regelgeving. De binnen de methode ontwikkelde kennisregels bieden ook het inzicht om enerzijds een uitspraak te doen over de autorisatiestructuur en anderzijds om zo nodig te komen tot een herontwerp van autorisatieregels en -matrices.

Administratieve organisatie

(Bron: http://nl.wikipedia.org/wiki/Administratieve_organisatie)

Administratieve Organisatie (AO) houdt zich bezig met het functioneren van de organisatie, de informatie die hieruit voortkomt en het complex van maatregelen om het functioneren en informeren naar wens te laten verlopen. Een deugdelijke AO is van belang om op de juiste wijze financiële verantwoording te kunnen afleggen en daardoor een goedkeurende accountantsverklaring te verkrijgen.

Functiescheiding wordt toegepast om te voorkomen dat er, door bovenmatige autorisaties, misbruik of oneigenlijk gebruik van gegevens of processen plaatsvindt, waardoor het resultaat van de organisatie negatief wordt beïnvloed. Controletechnische Functiescheiding vindt plaats door bepaalde 'risicovolle' handelingen af te splitsen en bij verschillende functionarissen onder te brengen. Dat geeft meteen de grens van controletechnische functiescheiding aan: tegen samenspanning is vrijwel geen kruid gewassen.

Access Governance

(Bron: *KPMG Compact 2010_03*)

Access Governance (AG) is een efficiënt proces waarbij op regelmatige basis met behulp van analytische tooling toegang binnen, tot en over applicaties en IT-platformen periodiek wordt beoordeeld.



Conclusie

De ontwerpregels van Starreveld bieden een generiek kader voor het vaststellen van autorisatieregels voor de uitvoering van bedrijfsprocessen. En daarmee zijn deze regels bij uitstek geschikt als basis voor het formuleren van het autorisatiebeleid. De vraag waarom iemand welke autorisaties krijgt, is op grond van de aloude leer van de AO te beantwoorden. En het is mogelijk om de AG business rules te modelleren op basis van de functiescheidingsprincipes van Starreveld.

Wat we daarnaast kunnen vaststellen is dat ook Identiteiten- en Autorisatie-beheer te beschrijven is in termen van functies zoals ontwikkeld binnen de AO-theorie.

Een nadere concretisering van de theorie van Starreveld naar moderne informatieverwerking zou voor de opstellers van autorisatieregels een nog beter handvat kunnen geven. Maar tot die tijd raden we aan om het oude boek toch weer uit de kast te halen. ●

Bronvermelding

- *KPMG 2: Compact 2010_3 'Facts to value, beyond application security'* van Francken, Hermans, Schreurs



- CoBIT 4.1, www.isaca.org
- *Bestuurlijke informatieverzorging Deel 1: algemene grondslagen (druk 5, 2002, ISBN-13: 9789020730524)* - R.W. Starreveld, O.C. van Leeuwen, H. van Nimwegen
- *Bestuurlijke informatieverzorging deel 2a (druk 5, 2004, ISBN-13: 9789020730531)* - R.W. Starreveld, O.C. van Leeuwen, H. van Nimwegen
- *Bestuurlijke informatieverzorging deel 2B (druk 5, 2008, ISBN-13: 9789020733105)* - R.W. Starreveld, O.C. van Leeuwen, H.B. de Mare



- *KPMG 1: Afweging tussen business-flexibiliteit en controle via functiescheiding* - Gerben de Roest en Maarten de Rooij (KPMG Compact, 2008-3, <http://www.compact.nl/artikelen/C-2008-3-Roest.htm>)